

CLAIMS

What is claimed is:

1. A probe apparatus for application monitoring, comprising:
 - (a) a data collection module for collecting data from a network segment;
 - (b) a flow processor coupled to the data collection module for classifying the collected data into a plurality of flows;
 - (c) a capture system coupled to the flow processor for filtering and buffering the collected data; and
 - (d) a main processor for processing the filtered data.
2. The probe apparatus as recited in claim 1, wherein the data collection module prepends the data with descriptor information, wherein the descriptor information is used by the capture system to filter the collected data.
3. The probe apparatus as recited in claim 1, wherein the capture system includes a capture buffer and a focus buffer, wherein the capture system filters the collected data stored in the capture buffer, wherein the filtered data is sent to the focus buffer.
4. The probe apparatus as recited in claim 3, wherein the capture system captures the collected data in the capture buffer in at least one of a fill and stop mode, a wrap mode, a priority queuing mode, and a non-priority queuing mode.

5. The probe apparatus as recited in claim 4, wherein in priority queuing mode the capture buffer is segmented into priority and non-priority queues, wherein the buffer space for each queue varies dynamically based on the arrival of data that meets priority criteria.
6. The probe apparatus as recited in claim 5, wherein buffers are reallocated to the priority queue from the non-priority queue as the number of priority flows increases.
7. The probe apparatus as recited in claim 5, wherein buffers are reallocated to the non-priority queue from the priority queue as the number of priority flows decreases.
8. The probe apparatus as recited in claim 5, wherein the capture system selectively discards flows from the priority queue based on predetermined criteria.
9. The probe apparatus as recited in claim 1, wherein the main processor identifies a flow as being important, wherein the flow processor uses the identification as criteria for forwarding additional data from the identified flow to the main processor.
10. The probe apparatus as recited in claim 1, wherein at least a portion of the probe apparatus is implemented on a Field Programmable Gate Array (FPGA).

11. The probe apparatus as recited in claim 10, wherein the portion of the probe apparatus implemented on the FPGA includes dedicated FPGA engines for capture and filtering of the data.
12. A method for application monitoring, comprising:
 - (a) collecting data from a network segment;
 - (b) classifying the collected data into a plurality of flows;
 - (c) filtering and buffering the collected data; and
 - (d) processing the filtered data.
13. The method as recited in claim 12, further comprising prepending the data with descriptor information, wherein the descriptor information is used to filter the collected data.
14. The method as recited in claim 12, further comprising storing the collected data in a capture buffer, filtering the collected data stored in the capture buffer, and sending the filtered data to a focus buffer.
15. The method as recited in claim 14, further comprising capturing the collected data in the capture buffer in at least one of a fill and stop mode, a wrap mode, a priority queuing mode, and a non-priority queuing mode.
16. The method as recited in claim 15, further comprising segmenting the capture buffer into priority and non-priority queues in priority queuing mode, wherein

the buffer space for each queue varies dynamically based on the arrival of data that meets priority criteria.

17. The method as recited in claim 16, further comprising reallocating buffers to the priority queue from the non-priority queue as the number of priority flows increases.
18. The method as recited in claim 16, further comprising reallocating buffers to the non-priority queue from the priority queue as the number of priority flows decreases.
19. The method as recited in claim 16, wherein the capture system selectively discards flows from the priority queue based on predetermined criteria.
20. The method as recited in claim 12, further comprising identifying a flow of data as being important, and using the identification as criteria for forwarding additional data from the identified flow for processing.
21. A computer program product for application monitoring, comprising:
 - (a) computer code for collecting data from a network segment;
 - (b) computer code for classifying the collected data into a plurality of flows;
 - (c) computer code for filtering and buffering the collected data; and
 - (d) computer code for processing the filtered data.

22. A probe apparatus for application monitoring, comprising:
- (a) a data collection module for collecting data from a network segment;
 - (b) a flow processor coupled to the data collection module for classifying the collected data into a plurality of flows;
 - (c) a capture system coupled to the flow processor for filtering and buffering the collected data, wherein the capture system includes a capture buffer and a focus buffer, wherein in priority queuing mode the capture buffer is segmented into priority and non-priority queues, wherein the buffer space for each queue varies dynamically based on the arrival of data that meets priority criteria; and
 - (d) a main processor for processing the filtered data.
23. A probe apparatus for application monitoring, comprising:
- (a) a data collection module for collecting data from a network segment;
 - (b) a flow processor coupled to the data collection module for classifying the collected data into a plurality of flows;
 - (c) a capture system coupled to the flow processor for filtering and buffering the collected data; and
 - (d) a main processor for processing the filtered data;
 - (e) wherein the data collection module prepends the data with descriptor information, wherein the descriptor information is used by the capture system to filter the collected data;
 - (f) wherein the capture system includes a capture buffer and a focus buffer, wherein the capture system filters the collected data stored in the capture buffer, wherein the filtered data is sent to the focus buffer;

- (g) wherein the capture system captures the collected data in the capture buffer in at least one of a fill and stop mode, a wrap mode, a priority queuing mode, and a non-priority queuing mode;
- (h) wherein in priority queuing mode the capture buffer is segmented into priority and non-priority queues, wherein the buffer space for each queue varies dynamically based on the arrival of data that meets priority criteria;
- (i) wherein buffers are reallocated to the priority queue from the non-priority queue as the number of priority flows increases;
- (j) wherein buffers are reallocated to the non-priority queue from the priority queue as the number of priority flows decreases;
- (k) wherein the capture system selectively discards flows from the priority queue based on predetermined criteria including at least one of an amount of priority data exceeding a processing capability of the system, user specifications, and the flow matching a randomly selected identifier;
- (l) wherein the main processor identifies a flow as being important, wherein the flow processor uses the identification as criteria for forwarding additional data from the identified flow to the main processor;
- (m) wherein at least a portion of the probe apparatus is implemented on a Field Programmable Gate Array (FPGA);
- (n) wherein the portion of the probe apparatus implemented on the FPGA includes dedicated FPGA engines for capture and filtering of the data.

2010-02-24